CyberArk Eliminates Security Gaps Across Public, Private, Hybrid Cloud and SaaS Environments

April 29, 2014 4:55 PM ET

Single Privileged Account Security Platform Secures Entire Spectrum of Privileged Accounts from On-premises to Cloud

Newton, Mass. â€“ April 29, 2014 â€“ CyberArk, the company securing the heart of the enterprise, today announced it has extended the CyberArk Privileged Account Security Solution to all major public, private, hybrid cloud and software as a service (SaaS) environments. By integrating with leading business, social media, IT and operational cloud solutions, CyberArk empowers customers to discover, monitor and secure privileged accounts across the entire IT infrastructure, protecting the primary pathway of all advanced attacks.

While privileged accounts have been implicated in 100 percent of advanced cyber-attack breaches[1], they largely go unprotected across cloud environments, due to immature defense strategies around this critical security layer. Hackers target these accounts because they provide the â€˜keys to controlling the infrastructure,â€™ â€“ whether that is through the cloud, on-premises, or across industrial control systems. The scalable, fluid infrastructure inherent in cloud environments results in unique differences in how privileged accounts behave.

Plugging this critical security gap, CyberArkâ€™s new cloud capabilities enable full monitoring and control over all privileged and administrative credentials that are uniquely required to manage cloud environments and hosted images. CyberArk is the only provider with a full solution-set, including behavioral analytics, covering the entire spectrum of privilege, including out of the box integrations with SaaS applications, hypervisor management solutions, as well as supporting major cloud platforms such as Amazon Web Services (AWS) and Microsoft Azure.

â€œThe cloud is fundamentally changing the nature of privileged account security. Server instances can be created instantaneously across multiple cloud environments, SaaS applications serve more critical functions, while infrastructure and privileged accounts are maintained in part by third-party vendors,â€ said Roy Adar, vice president, product management, CyberArk. â€œMigrating to the cloud introduces complexity for enterprises to navigate, which is why CyberArk has gone to great lengths to create a single, streamlined approach to manage privilege from the datacenter out to any cloud environment. No matter what environment an organizations uses, CyberArk has you covered.â€

Defending Against Advanced Threats in the Cloud

By extending its Privileged Account Security Solution to the cloud, CyberArk enables customers to use the same platform protecting on-premises and industrial control systems to cover their cloud environments, including:

Public Clouds: CyberArk integrates with all cloud providers and leading service providers like AWS and Azure empowering customers to:

- Use the same infrastructure to secure privileged access to on-site servers, databases, desktops, network device and remotely managed machines
- Prevent guest machines from exposing default password vulnerabilities
- Eliminate hard coded and visible credentials from applications and scripts that use cloud providersâ€™ API
- Establish single-sign-on to privileged accounts in the cloud
- Protect cloud-based servers from unauthorized access by third-party cloud service providers and malicious attackers
- Monitor all privileged user activity and alert on suspicious behavior in public cloud environments

Private Clouds: Integrations with VMware vCenter, and Microsoft HyperV provide:

- Improved security protection of management system credentials, including password rotation
- Automatic replacement of default passwords for newly provisioned systems and guest machines

- Monitoring, recording and alerting on all administrative user sessions for faster and more thorough compliance auditing

SaaS Environments: Applications provided as a service face a myriad of challenges with shared passwords. CyberArk provides integrations with leading SaaS applications, including Salesforce.com, Office365, Windows Intune, Facebook, Twitter, LinkedIn and Microsoft Dynamics CRM to:

- Automate and enforce best practice privileged account security, including enforcing one-time passwords
- Provide individual accountability fully monitoring activity on shared accounts
- Secure social media accounts from advanced attacks and privileged exploitation
- Provide single-sign-on to SaaS application accounts
- Extend privileged accounts security solution to all SaaS applications with the CyberArk universal connector

Additionally, to combat the significant increase in users accessing key accounts across cloud environments, CyberArk Privileged Threat Analytics analyzes all user behavior and detects activates anomalous to typical behavior. Behavior is analyzed in real-time, creating alerts for unusual activity, for example a user accessing a credential at an unusual time of day.

For more information on CyberArkâ€™s privileged account cloud security solutions, please visit www.cyberark.com.

About CyberArk

CyberArk is the only security company focused on eliminating the most advanced cyber threats; those that use insider privileges to attack the heart of the enterprise. Dedicated to stopping attacks before they stop business, CyberArk proactively secures against cyber threats before attacks can escalate and do irreparable damage. The company is trusted by the worldâ€™s leading companies â€“ including 30 of the Fortune 100 and 17 of the worldâ€™s top 20 banks â€“ to protect their highest value information assets, infrastructure and applications. A global company, CyberArk is headquartered in Petach Tikvah, Israel, with U.S. headquarters located in Newton, MA. The company also has offices throughout EMEA and Asia-Pacific. To learn more about CyberArk, visit www.cyberark.com, read the company blog, http://www.cyberark.com/blog/, follow on Twitter @CyberArk or Facebook at https://www.facebook.com/CyberArk.

---

[1] 2013 CyberSheath Report, APT Privileged Account Exploitation

Tuesday, April 29, 2014 - 09:15